

#2

PATENT  
81942.0011

Express Mail Label No. EL 713 695 963 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Junichi MURAKAMI

Serial No: Not assigned

Filed: January 22, 2001

For: COMMON KEY GENERATING METHOD,  
COMMON KEY GENERATOR,  
CRYPTOGRAPHIC COMMUNICATION  
METHOD AND CRYPTOGRAPHIC  
COMMUNICATION SYSTEM

Art Unit: Not assigned

Examiner: Not assigned



TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION  
Assistant Commissioner for Patents  
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016362 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 22, 2001

By: 

Louis A. Mok  
Registration No. 22,585  
Attorney for Applicant(s)

/500 South Grand Avenue, Suite 1900  
Los Angeles, California 90071  
Telephone: 213-337-6700  
Facsimile: 213-337-6701

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

jc862 U.S. PRO  
09/766807  
01/22/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年 1月25日

出 願 番 号  
Application Number:

特願2000-016362

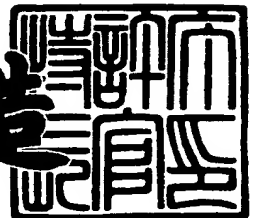
出 願 人  
Applicant(s):

村田機械株式会社  
笠原 正雄

2000年 8月18日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3064844

【書類名】 特許願

【整理番号】 20907

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00  
G09C 1/00

【発明の名称】 共通鍵生成方法、共通鍵生成器、暗号通信方法、暗号通信システム及びプログラムを記録した記録媒体

【請求項の数】 11

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 共通鍵生成方法、共通鍵生成器、暗号通信方法、暗号通信システム及びプログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする共通鍵生成方法。

【請求項 2】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項 1 に記載の共通鍵生成方法。

【請求項 3】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成器において、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段を備えることを特徴とする共通鍵生成器。

【請求項 4】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項 3 に記載の共通鍵生成器。

【請求項 5】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成

した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする暗号通信方法。

【請求項 6】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項 5 に記載の暗号通信方法。

【請求項 7】

前記センタは複数有り、複数の各センタが各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする請求項 5 又は 6 に記載の暗号通信方法。

【請求項 8】

センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信システムにおいて、各エンティティには、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段と、を備えたことを特徴とする暗号通信システム。

【請求項 9】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項 8 に記載の暗号通信システム。

【請求項 10】

コンピュータに、センタから送付された各エンティティ固有の秘密鍵と通信相手のエンティティの特定情報とから暗号通信に利用する共通鍵を生成させるため

のプログラムが記録されているコンピュータ読み取りが可能な記録媒体において、通信相手のエンティティの特定情報の構成要素に不足があるどうかの判断をコンピュータに実行させる第1プログラムコード手段と、前記通信相手のエンティティの特定情報の構成要素に不足があると判断された場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成させることをコンピュータに実行させる第2プログラムコード手段と、を含むことを特徴とするプログラムが記録されている記録媒体。

【請求項11】

前記特定情報は電子メールアドレスであり、構成要素の一部はドメイン名であることを特徴とする請求項10に記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、エンティティ間の暗号通信に利用される共通鍵を生成する共通鍵生成方法、共通鍵生成器、エンティティ間で暗号通信を行う暗号通信方法、暗号通信システム、及びそれらに用いられるプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換するこ

とである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

#### 【 0 0 0 4 】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用した D E S (Data Encryption Standard) はその典型例である。このような共通鍵暗号方式の従来例は、次のような 3 種の方法に分類できる。

#### 【 0 0 0 5 】

##### ① 第 1 の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法

##### ② 第 2 の方法

暗号通信の都度、呼び通信により鍵を共有し合う方法 (Diffie-Hellman による鍵共有方式、公開鍵方式による鍵配送方式等)。

##### ③ 第 3 の方法

各ユーザ (エンティティ) の氏名、住所等の個人を特定する公開された特定情報 (I D (Identity) 情報) を利用して、予備通信を行うことなく、送信側のエンティティ、受信側のエンティティが独立に同一の共通鍵を生成する方法 (K P S (Key Predistribution System)、I D - N I K S (ID-based Non-Interactive Key Sharing Schemes) 等)。

#### 【 0 0 0 6 】

第 1 の方法では、通信相手の共通鍵を保管しておく必要がある。また、第 2 の方法は、鍵共有のための予備通信が必要である。第 3 の方法は、通信相手の共通鍵を保管する必要もなく、予備通信も不要であり、公開された相手の I D 情報と



センタから予め配布されている固有の秘密パラメータとを用いて、必要時に、任意の相手との共通鍵を生成できるので、便利な方法である。

## 【0007】

図11は、このID-NIKSのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図11において、エンティティXの特定情報であるエンティティXの名前、住所、電話番号等のID情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(ID_X)$ で表す。センタは任意のエンティティXに対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティXのID情報 $h(ID_X)$ に基づいて、以下のように秘密鍵 $S_{Xi}$ を計算し、秘密裏にエンティティXへ配布する。

$$S_{Xi} = F_i(\{SC_i\}, \{PC_i\}, h(ID_X))$$

## 【0008】

エンティティXは他の任意のエンティティYとの間で、暗号化、復号のための共通鍵 $K_{XY}$ を、エンティティX自身の秘密鍵 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先のエンティティYのID情報 $h(ID_Y)$ を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

また、エンティティYも同様にエンティティXへの共通鍵 $K_{YX}$ を生成する。もし常に $K_{XY} = K_{YX}$ の関係が成立すれば、この鍵 $K_{XY}$ 、 $K_{YX}$ をエンティティX、Y間で暗号化鍵、復号鍵として使用できる。

## 【0009】

本発明者等は、このようなID-NIKSについて種々の暗号化方法、共通鍵生成方法、暗号通信方法等を提案しており、また、各エンティティのID情報を複数に分割して複数の各センタからその分割ID情報に基づく秘密鍵をエンティティに配布する構成にして、より安全性を高めるようにしたID-NIKSによる暗号化方法、共通鍵生成方法、暗号通信方法等についても、提案している。

## 【0010】

上記提案においては、ID情報として電子メールアドレスを使用し、各エンティティにおいて共通鍵を生成する際、各エンティティは各センタから発行された

各エンティティ固有の秘密鍵と通信相手となるエンティティの電子メールアドレスに基づいて、共通鍵を生成する。その共通鍵を使用して、送信時には平文を暗号化して暗号文を生成し、受信時には暗号文を復号して平文を再生する。

## 【0011】

## 【発明が解決しようとする課題】

各エンティティが、ドメイン名が付いている電子メールアドレスを自己の電子メールアドレスとして、秘密鍵登録を行っている、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、共通鍵を正しく生成できないので、暗号通信を行うことができない。

## 【0012】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合でも、確実に共通鍵を生成できる共通鍵生成方法及び暗号通信方法等を提供することを目的とする。

## 【0013】

## 【課題を解決するための手段】

本発明の共通鍵生成方法においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする。

## 【0014】

また、本発明の共通鍵生成器においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成する共通鍵生成器において、通

信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段を備えることを特徴とする。

## 【 0 0 1 5 】

また、本発明の暗号通信方法においては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信方法において、通信相手のエンティティの特定情報の構成要素に不足がある場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成することを特徴とする。

## 【 0 0 1 6 】

また、本発明の暗号通信システムにおいては、センタから各エンティティへ、各エンティティ固有の特定情報を利用して作成した各エンティティ固有の秘密鍵を送付し、各エンティティにおいて、前記センタから送付された前記秘密鍵と通信相手のエンティティの特定情報とから共通鍵を生成し、生成された共通鍵により暗号化及び復号を行う暗号通信システムにおいて、各エンティティには、通信相手のエンティティの特定情報の構成要素に不足があるかどうかを判断する手段と、前記判断手段が、前記通信相手のエンティティの特定情報の構成要素に不足があると判断した場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成する生成手段と、を備えたことを特徴とする。

## 【 0 0 1 7 】

また、本発明のコンピュータ読み取りが可能な記録媒体においては、コンピュータに、センタから送付された各エンティティ固有の秘密鍵と通信相手のエンティティの特定情報とから暗号通信に利用する共通鍵を生成させるためのプログラ

ムが記録されているコンピュータ読み取りが可能な記録媒体において、通信相手のエンティティの特定情報の構成要素に不足があるどうかの判断をコンピュータに実行させる第1プログラムコード手段と、前記通信相手のエンティティの特定情報の構成要素に不足があると判断された場合には、自己の特定情報の構成要素の一部を、前記通信相手のエンティティの特定情報に追加してから、共通鍵を生成させることをコンピュータに実行させる第2プログラムコード手段と、を含むことを特徴とする。

【0018】

また、上記の発明において、前記特定情報は電子メールアドレスであり、前記構成要素の一部はドメイン名であることを特徴とする。

【0019】

また、上記の発明において、前記センタは複数有り、複数の各センタが各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を発行することを特徴とする。

【0020】

本発明では、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、自己の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するので、確実に共通鍵を生成することができる。

【0021】

#### 【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（K個）のセンタ1が、秘密鍵発行のサーバとして設定されている。なお、これらのセンタ1としては、例えば社会の公的機関を想定できる。

【0022】

これらの各センタ1と、この暗号通信システムを利用するユーザとしての複数の各エンティティ  $a, b, \dots, z$  とは、通信路  $2_{a1}, \dots, 2_{aK}, 2_{b1}, \dots, 2_{bK}, \dots, 2_{z1}, \dots, 2_{zK}$  により接続されており、これらの通信路を介して、各

エンティティ a, b, …, z から各センタ 1 へ秘密鍵発行の依頼がなされ、各センタ 1 から各エンティティ固有の秘密鍵が各エンティティ a, b, …, z へ発行されるようになっている。また、2 人のエンティティ間には電子メールによる通信路  $3_{ab}$ ,  $3_{az}$ ,  $3_{bz}$ , … が設けられており、通信情報を暗号化した暗号文が互いのエンティティ間で電子メールにより送受信されるようになっている。

### 【0023】

図 2 は、2 人のエンティティ a, b 間における情報の通信状態を示す模式図である。図 2 の例は、エンティティ a が平文（メッセージ）M を暗号文 C に暗号化してそれをエンティティ b へ送信し、エンティティ b がその暗号文 C を元の平文（メッセージ）M に復号する場合を示している。

### 【0024】

総数 K 個の各センタ 1 には、自身の秘密情報（対称行列）から各エンティティ a, b 毎に選択したものを各エンティティのパスワードに基づいて暗号化して各エンティティ a, b 固有の秘密鍵を発行する秘密鍵発行器 2 が備えられている。秘密鍵発行器 2 は、その内部構成を示す図 3 に表すように、暗号化された秘密情報を格納する秘密情報格納部 3 と、秘密情報格納部 3 に格納されている暗号化秘密情報を読み出して復号する秘密情報復号部 4 と、センタ 1 自身の秘密情報と各エンティティ a, b の特定情報（ID 情報）から各エンティティ a, b 固有の秘密鍵を作成する秘密鍵作成部 5 と、作成された秘密鍵を各エンティティ a, b から入力されたパスワードで暗号化する秘密鍵暗号化部 6 と、所定周期毎に更新されるセンタ 1 の秘密情報を暗号化して秘密情報格納部 3 に書き込む秘密情報更新部 6 とを有する。

### 【0025】

エンティティ a 側には、K 個の各センタ 1 に対して秘密鍵の発行を要求する登録部 10 と、K 個の各センタ 1 から送られる秘密鍵方式でのエンティティ a 自身固有の秘密鍵を復号する第 1 秘密鍵復号部 11 と、復号された K 個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部 12 と、暗号化された秘密鍵を格納する秘密鍵格納部 13 と、秘密鍵格納部 13 に格納されている暗号化秘密鍵を読み出して復号する第 2 秘密鍵復号部 14 と、自身固有の秘密鍵とエンティティ b の特定情

報（ID情報）とに基づいてエンティティ a が求めるエンティティ b との共通鍵  $K_{ab}$  を生成する共通鍵生成部 15 と、共通鍵  $K_{ab}$  を用いて平文（メッセージ）M を暗号文 C に暗号化して電子メールによる通信路 30 へ出力する平文暗号化部 16 と、共通鍵、平文、暗号文等を表示する表示部 17 とが備えられている。

## 【0026】

また、エンティティ b 側には、K 個の各センタ 1 に対して秘密鍵の発行を要求する登録部 20 と、K 個の各センタ 1 から送られる秘密鍵方式でのエンティティ b 自身固有の秘密鍵を復号する第 1 秘密鍵復号部 21 と、復号された K 個の自身固有の秘密鍵を暗号化する秘密鍵暗号化部 22 と、暗号化された秘密鍵を格納する秘密鍵格納部 23 と、秘密鍵格納部 23 に格納されている暗号化秘密鍵を読み出して復号する第 2 秘密鍵復号部 24 と、自身固有の秘密鍵とエンティティ a の特定情報（ID情報）とに基づいてエンティティ b が求めるエンティティ a との共通鍵  $K_{ba}$  を生成する共通鍵生成部 25 と、共通鍵  $K_{ba}$  を用いて通信路 30 から入力した暗号文 C を平文（メッセージ）M に復号して出力する暗号文復号部 26 と、共通鍵、平文、暗号文等を表示する表示部 27 とが備えられている。

## 【0027】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

## 【0028】

（予備処理）

各エンティティを特定する特定情報（ID情報）、例えばそのエンティティの電子メールアドレスを表す ID ベクトル（L ビット 2 進ベクトル）を、図 4 に示すように、ブロックサイズ M ビット毎に K 個のブロックに分割する。例えば、エンティティ a の電子メールアドレスを示す ID ベクトル（ベクトル  $I_a$ ）を式（1）のように分割する。分割特定情報である各ベクトル  $I_{aj}$ （ $j = 1, 2, \dots, K$ ）を分割 ID ベクトルと呼ぶ。なお、エンティティの電子メールアドレスが、ハッシュ関数によって L ビットの ID ベクトルに変換される。

## 【0029】

【数 1】

$$\overrightarrow{I_a} = [\overrightarrow{I_{a1}} | \overrightarrow{I_{a2}} | \cdots | \overrightarrow{I_{aK}}] \cdots (1)$$

【0030】

(秘密鍵発行処理 (エンティティの登録処理))

図5及び図6に、エンティティ a, b の登録部 10、20 によるセンタへの登録処理及び、各センタ 1 の秘密鍵発行器 2 による秘密鍵発行処理を示す。この暗号通信システムに参加したいエンティティ a, b、即ち、自身固有の秘密鍵の発行を希望するエンティティ a, b は、各センタ 1 (センタ第 1、第 2、・・・、第 K) へ登録し、秘密鍵を入手する。

【0031】

まず、図5 (I) に示すように、エンティティ a では、基本パスワードと自身の電子メールアドレスを登録部 10 へ入力する (S111)。登録部 10 は、基本パスワードと一方向性変換関数に基づいて、センタ第 1 用のパスワードを生成し (S112)、センタ第 1 への登録処理を行い、センタ第 1 から秘密鍵を入手する (S113)。

【0032】

同様に、それぞれ異なる一方向性変換関数を用いて、センタ第 2 用、センタ第 K 用のパスワードを生成し、センタ第 2、センタ第 K への登録処理を行い、秘密鍵を入手する (S114～S117)。同様に、図5 (II) に示すように、エンティティ b においても、登録部 20 により各センタ 1 への登録処理を行い、各センタ 1 から秘密鍵を入手する (S121～127)。

【0033】

次に、図6を参照しながら、エンティティ a におけるセンタ第 1 への登録処理及びセンタ第 1 におけるエンティティ a の秘密鍵発行処理について説明する。他のエンティティにおける登録処理及び他のセンタにおける秘密鍵発行処理についても同様である。

【0034】

エンティティ a の登録部 10 では、S112 で生成されたセンタ第 1 用のパス

ワードを取り込み（S211）、センタ第1のホームページにアクセスしてサーバを介して、パスワードとエンティティ a 自身の電子メールアドレスとを公開鍵方式（SSL等）で暗号化しセンタ第1へ送信する（S212, S213）。

【0035】

センタ第1の秘密鍵発行器2では、秘密情報格納部3に格納されている暗号化秘密情報を秘密情報復号部4で復号した秘密情報（後述する対称行列）を得る（S221）。また、エンティティ a から公開鍵方式で暗号化されたパスワードと電子メールアドレスを受信し（S222）、復号する（S223）。秘密鍵作成部5にて、エンティティ a の電子メールアドレスから得られた分割IDベクトルに対応する部分を選択し、エンティティ a の秘密鍵（後述する秘密鍵ベクトル）を生成する（S224）。

【0036】

生成した秘密鍵（秘密鍵ベクトル）をエンティティ a から受信したパスワードに基づいて暗号化して（S225）、即ち、選択した秘密鍵（秘密鍵ベクトル）にパスワードを盛り込んだ秘密鍵方式で、そのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する（S226）。この際の秘密鍵方式としては、DESを利用できる。なお、エンティティの電子メールアドレスを暗号化して送付するようにしても良い。

【0037】

エンティティ a は、暗号化されたエンティティ a の秘密鍵（秘密鍵ベクトル）を受信し（S214）、パスワードを用い、第1秘密鍵復号部11で復号する（S215）。さらに、復号した秘密鍵（秘密ベクトル）は安全のため、一旦、秘密鍵暗号化部12で暗号化されて（S216）、秘密鍵格納部13に格納される。

【0038】

同様にしてエンティティ a は、センタ第2、・・・、第Kへ登録を行い、秘密鍵を入手する。上述のように、各センタ1によって発行された各エンティティの秘密鍵（秘密鍵ベクトル）は、パスワードによって各センタ1で暗号化されてから各エンティティへ送付され、各エンティティで復号されるので、各エンティティ



は秘密鍵（秘密鍵ベクトル）を秘密裡に入手することができる。

【0039】

安全のためには、各センタ1毎にそれぞれ固有のパスワードを送付することが望ましいが、パスワードの管理が煩雑になる可能性がある。そこで、1つの基本パスワードと一方向性変換関数に基づいて、複数のパスワードを生成することにより、管理が必要なパスワード数を削減することができる。また、一方向性変換関数を秘密にすることにより、安全性が損なわれることはない。

【0040】

1つの基本パスワードと一方向性変換関数に基づいて複数のパスワードを生成するには、次のような方法がある。

- ①各センタ1毎に異なる一方向性変換関数を使用する。
- ②基本パスワードに各センタ毎に異なるスクランブル処理を施したり、各センタ毎に連番を付加するなどしてから、各センタ1で共通又は各センタ1毎に異なる一方向性変換関数を使用する。

【0041】

また、一方向性変換関数として一方向性ハッシュ関数を用いることができる。一方向性ハッシュ関数による演算後のパスワードは、元の基本パスワードよりデータ長が短くなるので、不都合であれば、適宜、異なる複数の一方向性ハッシュ関数による演算結果を組み合わせるパスワードを構成する。このようにすれば、一方向性ハッシュ関数による、データ長の低減を補うことができる。

【0042】

なお、より簡易的に、電子メールにより、エンティティの登録処理及び秘密鍵の発行処理を行うことも可能である。この場合、自身固有の秘密鍵の発行を希望するエンティティは、自身のパスワードを電子メールにて直接各センタ1へ公開鍵方式で送る。各センタ1では、上記の場合と同様に、秘密情報からエンティティに対応して選択した秘密鍵にエンティティ側で入力されたパスワードを盛り込んだ秘密鍵方式（DES等）でそのエンティティ固有の秘密鍵を、電子メールを介してそのエンティティに発行する。

【0043】

なお、上述した例では、電子メールにて秘密鍵を発行するようにしているが、ICカード等の可搬型の記録媒体にエンティティ固有の秘密鍵を書き込み、その記録媒体をエンティティへ送るようにすることも可能である。

## 【0044】

ここで、各センタ1での秘密情報（対称行列）、及び、各エンティティ固有の秘密鍵（秘密鍵ベクトル）の具体的内容について説明する。 $j$  ( $j = 1, 2, \dots, K$ ) 番目のセンタ1は、秘密情報として、ランダムな数を要素とする対称行列  $H_j$  ( $2^M \times 2^M$ ) を有している。そして、エンティティ  $a$  に対して、対称行列  $H_j$  のそのエンティティの分割IDベクトルに対応する行ベクトルを秘密鍵（秘密鍵ベクトル）として発行する。即ち、エンティティ  $a$  に対しては、 $H_j$  [ベクトル  $I_{aj}$ ] を発行する。この  $H_j$  [ベクトル  $I_{aj}$ ] は、対称行列  $H_j$  よりベクトル  $I_{aj}$  に対応した行を1行抜き出したベクトルを表す。

## 【0045】

ここで、エンティティ側でのパスワード入力の例について説明する。パスワード入力処理については、パスワード入力が不慣れなエンティティにとって特に、次のような2つの例が好適である。

## 【0046】

一方の例では、各エンティティが文字列を入力し、その入力データをbase64でエンコードしたものをパスワードとする。この場合、64種の各1つの文字入力にて6ビットのデータを表せるので、パスワードが64ビットである場合には、11個の文字を入力すれば良いことになる。

## 【0047】

また、他方の例では、0～9及びA～Fの16種の文字を入力することを原則として、これらの16種の文字以外が入力された場合には、その文字を0～9、A～Fの何れかの文字に置換する。

## 【0048】

（エンティティ  $a$ 、 $b$  における共通鍵の生成処理）

エンティティ  $a$ 、 $b$  における共通鍵生成処理について、図7を参照しながら説明する。エンティティ  $a$ （エンティティ  $b$ ）は、通信相手であるエンティティ  $b$

(エンティティ a) との共通鍵  $K_{ab}$  ( $K_{ba}$ ) を生成する際に、暗号化された秘密鍵 (秘密鍵ベクトル) を秘密鍵格納部 13 (23) から読み出して、第2秘密鍵復号部 14 (24) で再び秘密鍵 (秘密鍵ベクトル) を復号する (S311 (S321))。

## 【0049】

エンティティ a (エンティティ b) は、共通鍵を生成するために相手のエンティティ b (エンティティ a) の特定情報 (ID 情報) としての電子 f を必要とする。送信側となるエンティティ a においては、エンティティ b の電子メールアドレスは送信相手先の電子メールアドレスとして与えられる。また、受信側となるエンティティ b においては、エンティティ a の電子メールアドレスは受信した電子メールの発信元情報 (From フィールド等) から得ることができる (S322)。

## 【0050】

共通鍵生成部 15 (25) にて、各センタ 1 から受け取った秘密鍵 (秘密鍵ベクトル) のうち、エンティティ b (エンティティ a) の特定情報 (ID 情報) に基づいて、対応する要素を取り出し、これら K 個の要素を合成して、エンティティ a (エンティティ b) のエンティティ b (エンティティ a) に対する共通鍵  $K_{ab}$  ( $K_{ba}$ ) を生成する (S312 (S323))。ここで、K 個の各センタが有する秘密情報 (行列) の対称性に基づいて、両共通鍵  $K_{ab}$ ,  $K_{ba}$  は一致する。

## 【0051】

エンティティ a, b の特定情報 (ID 情報) として、電子メールアドレスを利用している。図 8 に示すように、電子メールアドレスはメールシステムによって、ドメイン名が付いているもの (図 8 (I)) と、付いていないもの (図 8 (II)) がある。ドメイン名が付いている電子メールアドレスはインターネットの電子メールアドレスとして使用されている。また、インターネット以外のメールシステムにおいては、ドメイン名が付いていない電子メールアドレスを使用していることもある。

## 【0052】

ゲートウェイを介してインターネットに接続された LAN 環境においては、こ

れら 2 種類の電子メールアドレスのいずれでも使用できる場合がある。例えば、LAN などの閉じた範囲では、いずれの電子メールアドレスでも使用可能であり、ゲートウェイを介してインターネットメールを使用する場合には、ドメイン名が付いている電子メールアドレスを使用するようになっている。

## 【 0 0 5 3 】

エンティティ a, b においては、インターネットの電子メールにより、各センタから秘密鍵（秘密鍵ベクトル）を入手した場合には、ドメイン名が付いている電子メールアドレスに基づいて秘密鍵（秘密鍵ベクトル）が生成されている。したがって、共有鍵を生成する相手の電子メールアドレスにドメイン名が付いていなければ、共通鍵を正しく生成できなくなり、暗号通信を行うことができない。

## 【 0 0 5 4 】

そこで、図 9 (I) 及び図 9 (II) に示すように、送信側となるエンティティ a において、相手先として指定されたエンティティ b の電子メールアドレスにドメイン名が付いていない場合には (S 4 1 1)、エンティティ a と同じドメイン名を付けて (S 4 1 2)、共通鍵  $K_{ab}$  の生成を行うようにした (S 4 1 3)。

## 【 0 0 5 5 】

また、受信側となるエンティティ b において、エンティティ a から受信した電子メールの発信元情報 (From フィールド) 等の電子メールアドレスに、ドメイン名が付いていない場合には (S 4 2 1)、エンティティ b と同じドメイン名を付けて (S 4 2 2)、共通鍵  $K_{ba}$  の生成を行うようにした (S 4 2 3)。

## 【 0 0 5 6 】

(エンティティ a における暗号化処理、エンティティ b における復号処理)

図 7 に戻り、エンティティ a にあって、共通鍵生成部 1 5 で生成された共通鍵  $K_{ab}$  を用いて、平文暗号化部 1 6 にて、平文 (メッセージ) M が暗号文 C に暗号化されて (S 3 1 3)、その暗号文 C が電子メールによる通信路 3 0 へ送信される (S 3 1 4)。エンティティ b にあって、共通鍵生成部 2 5 で生成された共通鍵  $K_{ba}$  を用いて、暗号文復号部 2 6 にて、暗号文 C が元の平文 (メッセージ) M に復号される (S 3 2 4)。

## 【 0 0 5 7 】

図 1 0 は、本発明の記録媒体の実施例の構成を示す図である。ここに例示するプログラムは、秘密鍵の発行をセンタへ依頼する登録処理、各エンティティからの依頼に基づいて各センタにおいて各エンティティ固有の秘密鍵を発行する上述したような秘密鍵発行処理、各センタから秘密鍵方式で発行された秘密鍵を各エンティティにおいて復号する上述したような秘密鍵復号処理、自身固有の秘密鍵を用いて通信相手との間の共通鍵を生成する上述したような共通鍵作成処理、センタの秘密情報（対称行列）、各エンティティの秘密鍵（秘密鍵ベクトル）を暗号化して格納する上述したような秘密情報、秘密鍵の格納・更新処理、共通鍵、平文、暗号文を表示する上述したような表示処理、及び／または、平文の暗号化処理、暗号文の復号処理等を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ 4 0 は、各ホスト側または各エンティティ側に設けられている。

#### 【 0 0 5 8 】

図 1 0 において、コンピュータ 4 0 とオンライン接続する記録媒体 4 1 は、コンピュータ 4 0 の設置場所から隔たって設置される例えば WWW (World Wide Web) のサーバコンピュータを用いてなり、記録媒体 4 1 には前述の如きプログラム 4 1 a が記録されている。記録媒体 4 1 から読み出されたプログラム 4 1 a がコンピュータ 4 0 を制御することにより、少なくとも 1 つの上記処理を実行する。

#### 【 0 0 5 9 】

コンピュータ 4 0 の内部に設けられた記録媒体 4 2 は、内蔵設置される例えばハードディスクドライブまたは ROM 等を用いてなり、記録媒体 4 2 には前述の如きプログラム 4 2 a が記録されている。記録媒体 4 2 から読み出されたプログラム 4 2 a がコンピュータ 4 0 を制御することにより、少なくとも 1 つの上記処理を実行する。

#### 【 0 0 6 0 】

コンピュータ 4 0 に設けられたディスクドライブ 4 0 a に装填して使用される記録媒体 4 3 は、運搬可能な例えば光磁気ディスク、CD-ROM またはフレキシブルディスク等を用いてなり、記録媒体 4 3 には前述の如きプログラム 4 3 a が記録されている。記録媒体 4 3 から読み出されたプログラム 4 3 a がコンピュ

ータ 4 0 を制御することにより、少なくとも 1 つ以上の上記処理を実行する。

【 0 0 6 1 】

【発明の効果】

以上詳述したように、本発明では、各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、自身の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するようにした。操作ミスやメールシステムにより、通信相手の電子メールアドレスにドメイン名が付かないような場合でも、共通鍵を生成することができる。

【図面の簡単な説明】

【図 1】

本発明の暗号通信システムの構成を示す模式図である。

【図 2】

2 個のエンティティ間における情報の通信状態を示す模式図である。

【図 3】

秘密鍵発行器の内部構成を示す図である。

【図 4】

エンティティの ID ベクトル（特定情報）分割例を示す模式図である。

【図 5】

エンティティにおける登録処理を示す流れ図である。

【図 6】

エンティティにおける登録処理及びセンタにおける秘密鍵発行処理を示す流れ図である。

【図 7】

エンティティ間における共通鍵生成及処理、暗号化処理及び復号処理を示す流れ図である。

【図 8】

電子メールアドレスの例を示す図である。

【図 9】

共通鍵生成処理を示す流れ図である。

【図 1 0】

記録媒体の実施例の構成を示す図である。

【図 1 1】

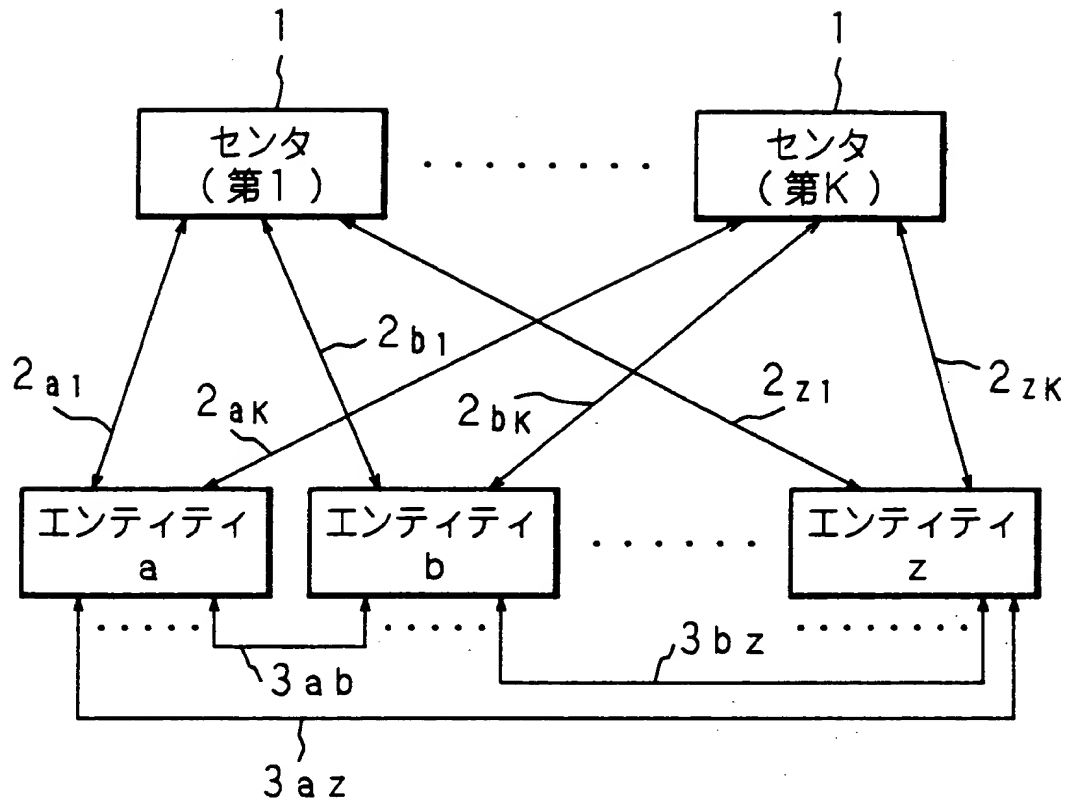
I D - N I K S のシステムの原理構成図である。

【符号の説明】

- 1 センタ
- 2 秘密鍵発行器
- 5 秘密鍵生成部
- 1 0, 2 0 秘密鍵登録部
- 1 5, 2 5 共通鍵生成部
- 1 6 平文暗号化部
- 2 6 暗号文復号部
- 3 0 通信路
- 4 0 コンピュータ
- 4 1, 4 2, 4 3 記録媒体
- a, b, z エンティティ

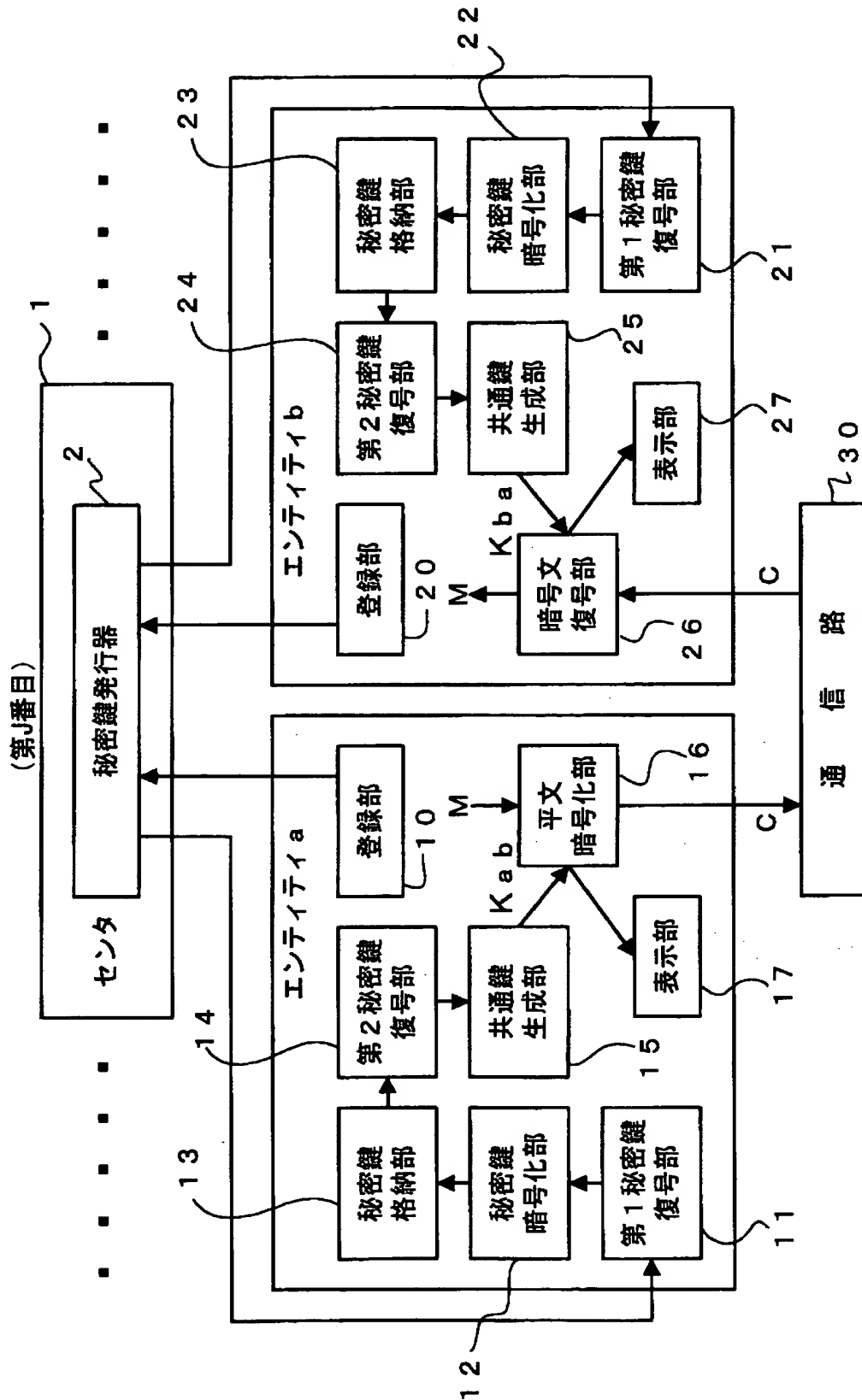
【書類名】 図面

【図1】

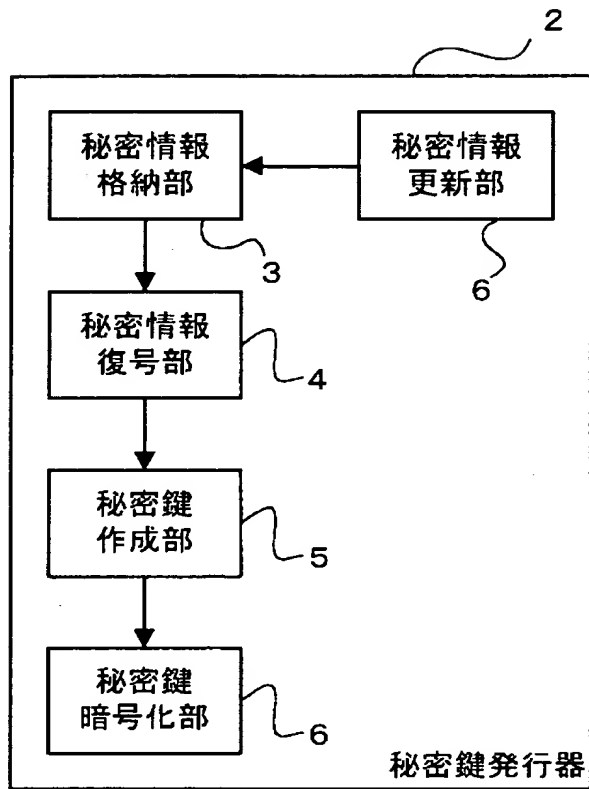




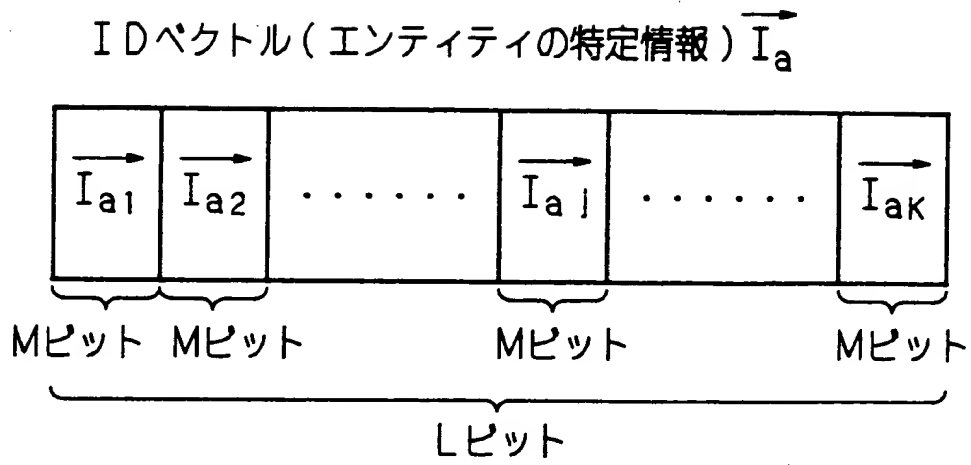
【図 2】



【図 3】

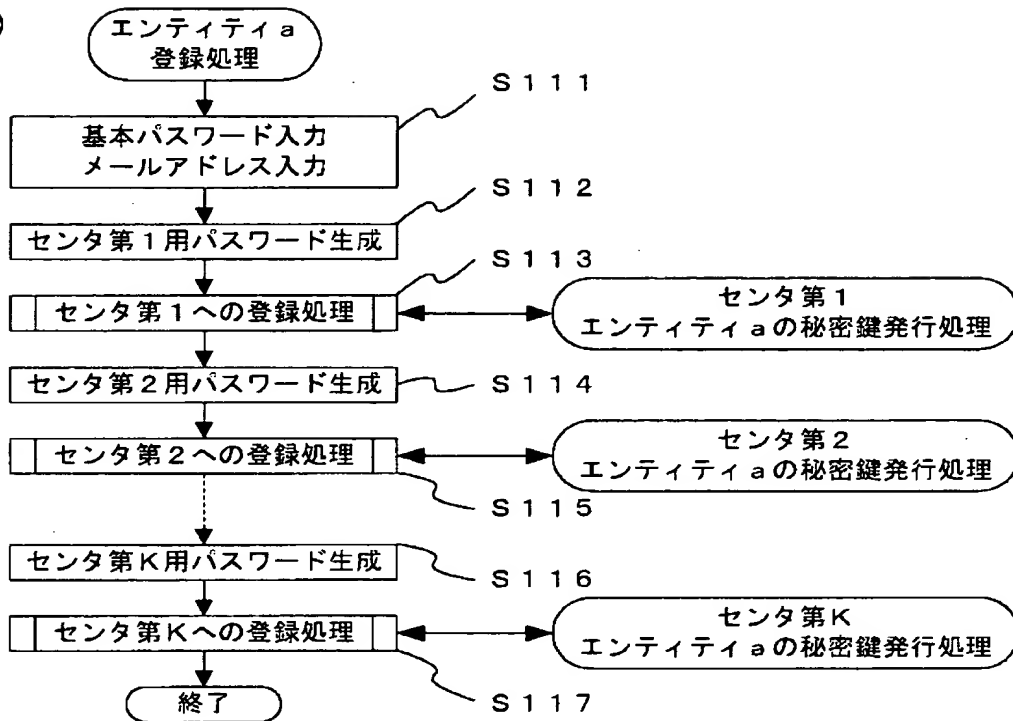


【図 4】

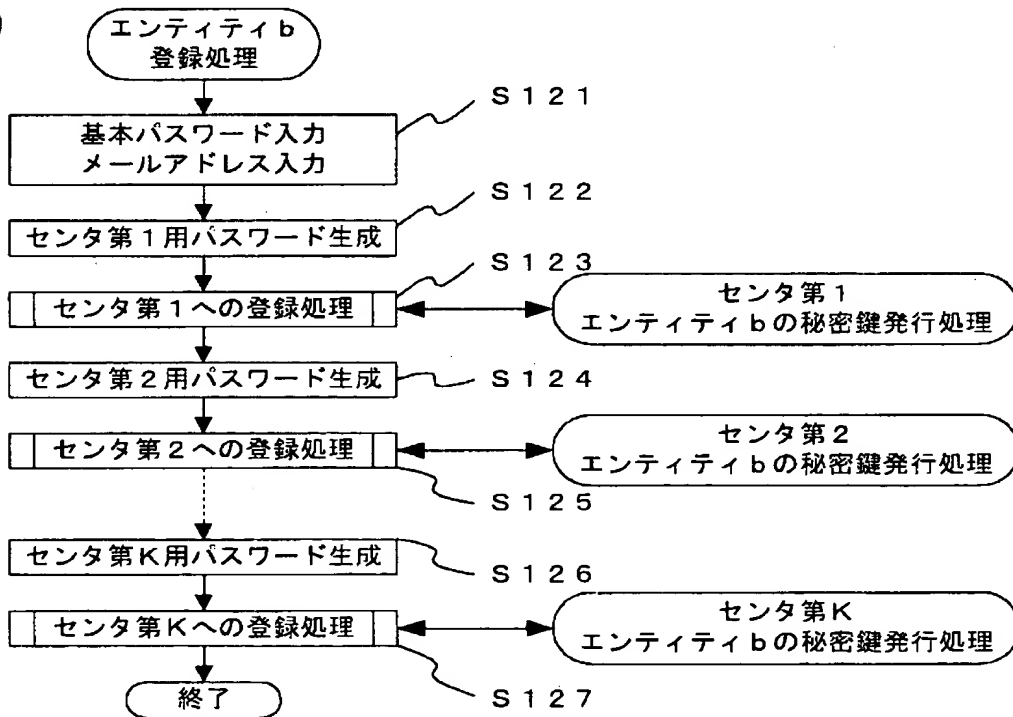


【図 5】

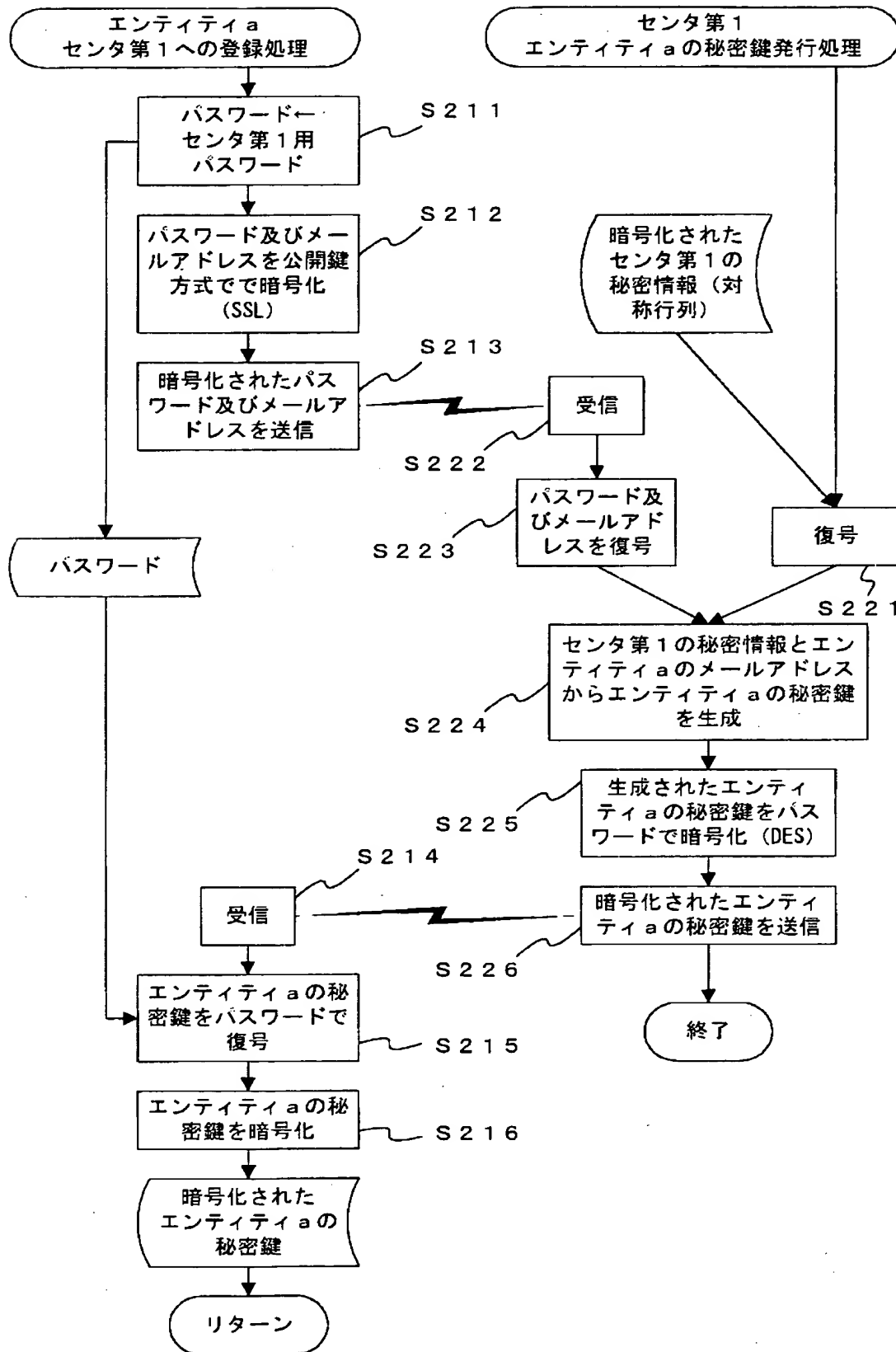
(I)



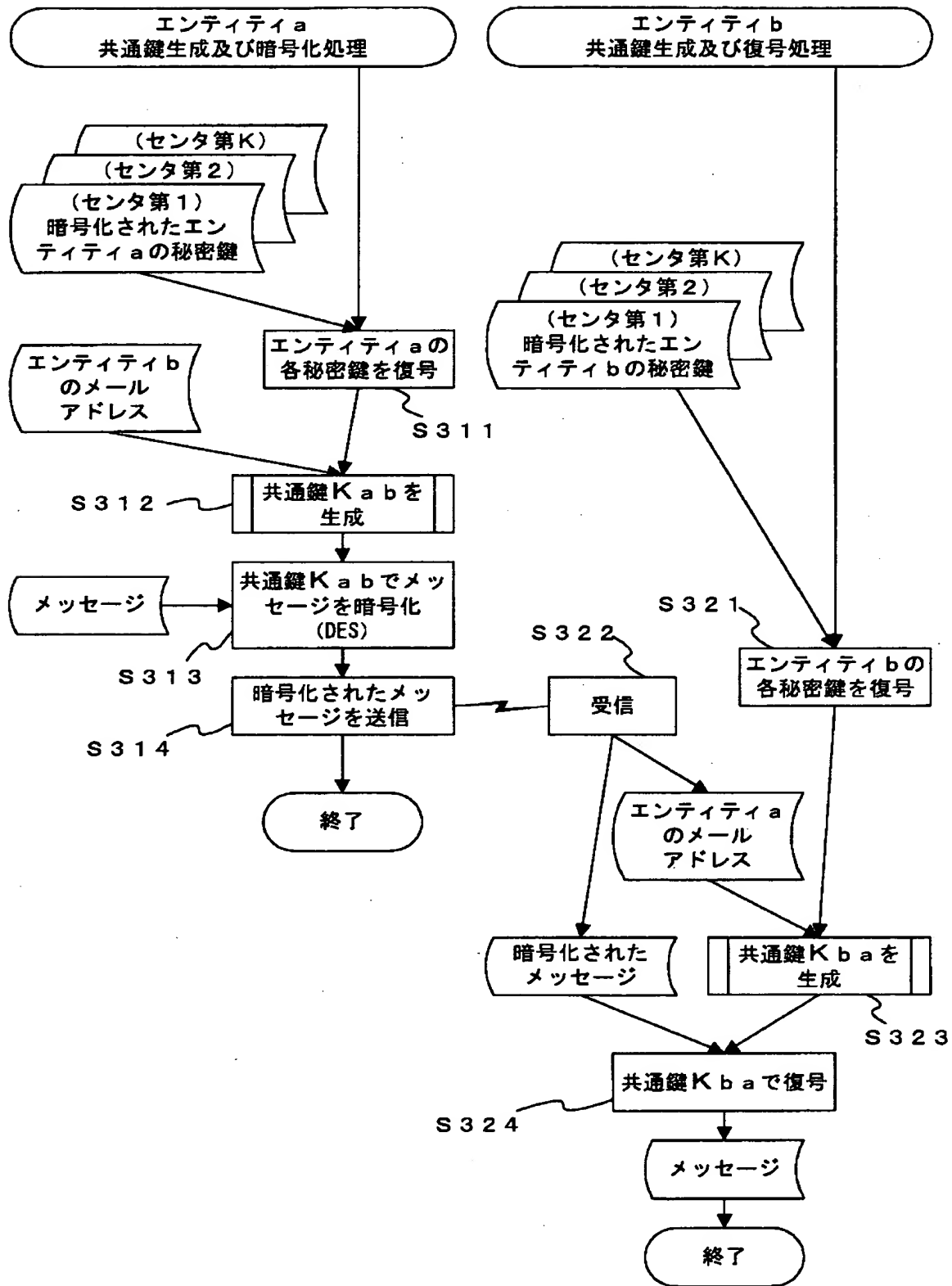
(II)



【図 6】



【図 7】



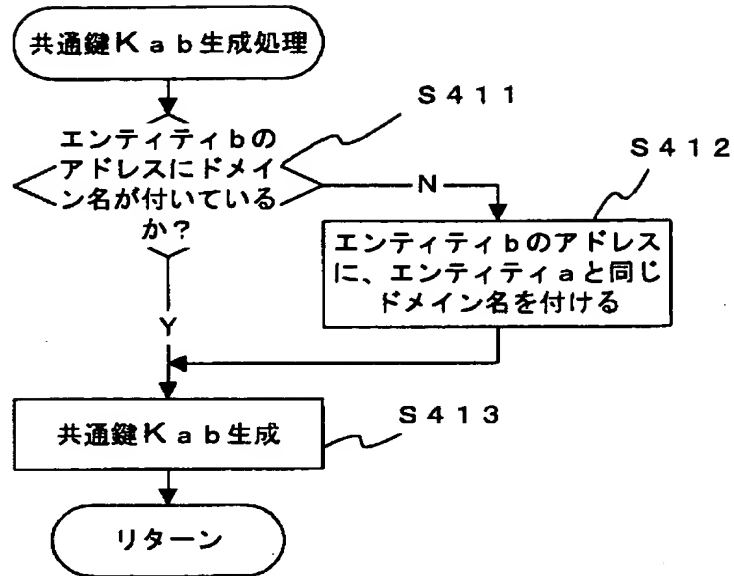
【図 8】

メールアドレスの例

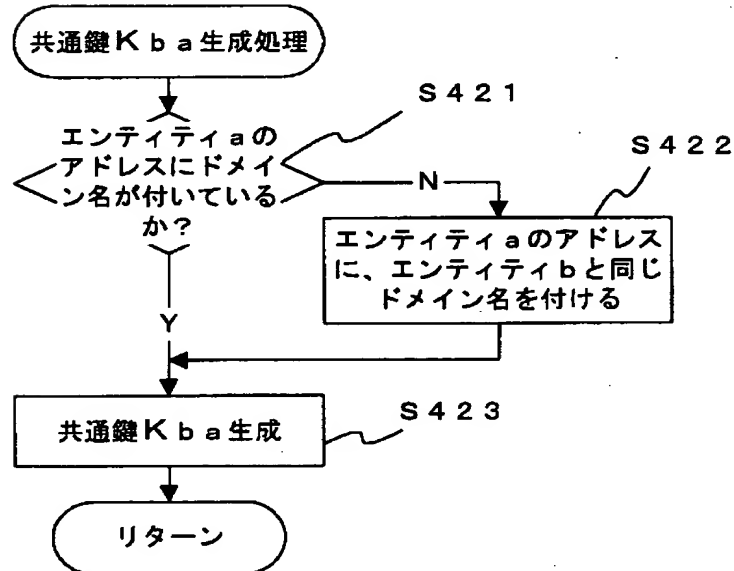
- |                       |                           |
|-----------------------|---------------------------|
| ( I ) ドメイン名が付いている場合   | thomas@xyz.co.jp<br>ドメイン名 |
| ( II ) ドメイン名が付いていない場合 | thomas                    |

【図 9】

(I)

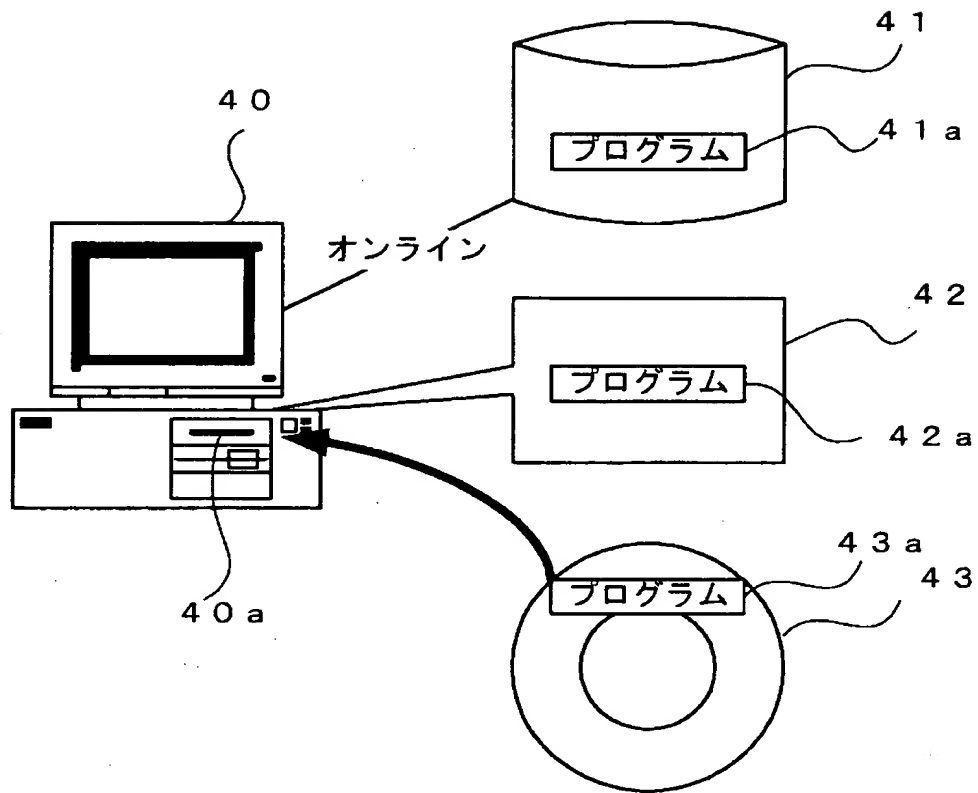


(II)

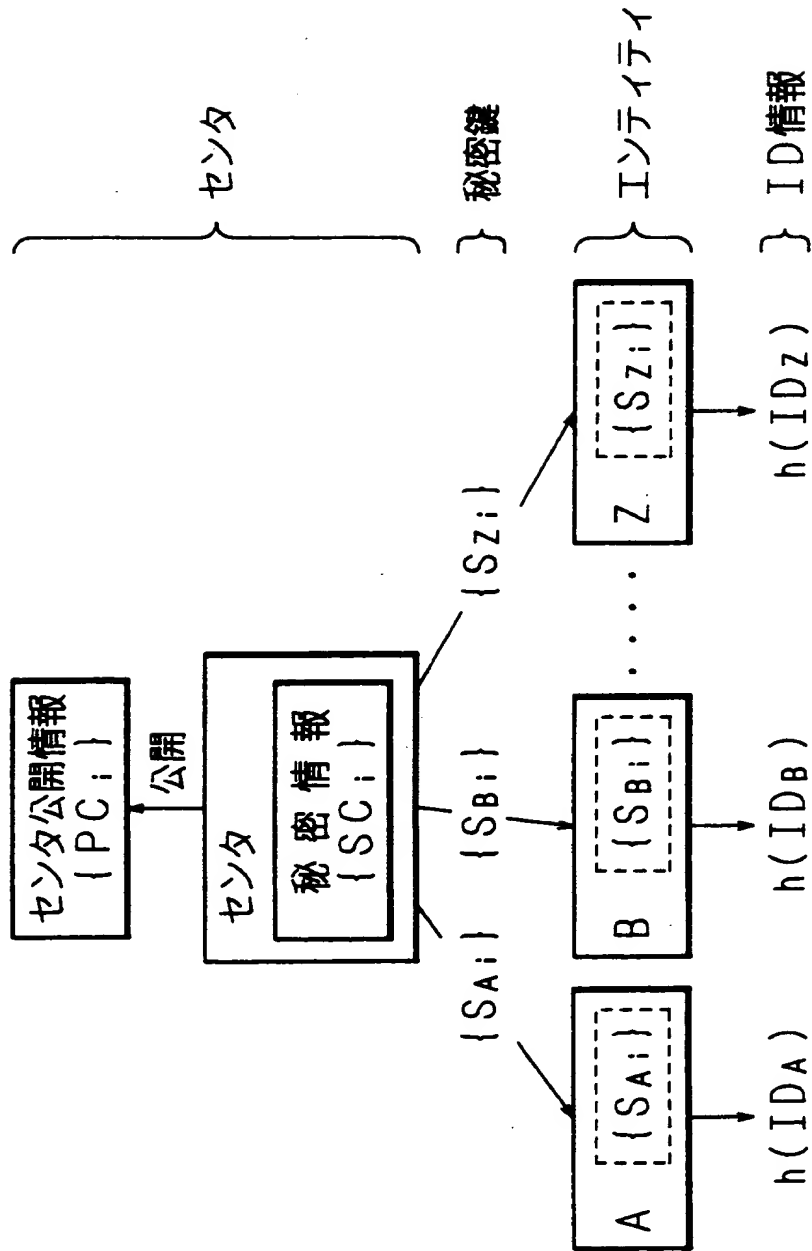




【図10】



【図 11】



【書類名】 要約書

【要約】

【課題】 ID-NIKSにおいて、ID情報として電子メールアドレスを使用した場合に、確実な共通鍵生成を行う。

【解決手段】 各エンティティにおける共通鍵生成時に、通信相手の電子メールアドレスにドメイン名が付いていないような場合には、共通鍵を正しく生成できないので、自身の電子メールアドレスのドメイン名と同じドメイン名を、相手の電子メールアドレスに付けてから共通鍵を生成するようにした。

【選択図】 図9

認定・付加情報

特許出願の番号	特願 2000-016362
受付番号	50000073742
書類名	特許願
担当官	宇留間 久雄 7277
作成日	平成 12 年 6 月 15 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町 3 番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市栗生外院 4 丁目 15 番 3 号
【氏名又は名称】	笠原 正雄

【復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 英仁

【代理人】

【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 登夫

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地

氏 名 村田機械株式会社

出 願 人 履 歷 情 報

識別番号 [597008636]

1. 変更年月日	1997年 1月21日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院4丁目15番3号
氏 名	笠原 正雄